REMARKS

Claims 1-40 are pending in the application. Claims 1-40 were rejected. Claims 1, 7, 21, and 27 are the independent claims. Reconsideration of the amended application is respectfully requested.

The Examiner required a drawing illustrating the claimed invention. Drawing figures are submitted herewith. On approval of the drawings by the Examiner, the written description will be amended accordingly.

The Examiner rejected claims 1-6 and 21-26 under 35 USC §103(a) as being unpatentable over Lipner et al.

Independent claim 1 recites a method of encrypting an object. According to the recited method, a plurality of key splits is combined to generate a cryptographic key. A cryptographic algorithm is initialized with the cryptographic key. The initialized cryptographic algorithm is applied to the object, to form an encrypted object. At least one of the plurality of key splits corresponds at least in part to a biometric measurement.

The Examiner cited Lipner et al. as disclosing that a plurality of key splits is combined to generate a cryptographic key, citing column 15, lines 13-16. This passage discusses a multiple split session key, referring to Fig. 13, which shows the flow of a sending program. According to this program, a secret session key KS is negotiated and formed, and then used to encrypt a message M. It is not disclosed that this key is formed through the combination of key splits. After encryption of the message, the session key is split into multiple parts. The example mentions splitting the key into two halves KS1 and KS2. See column 14, lines 55-66. These are the split session keys mentioned in the passage cited by the Examiner.

Thus, claim 1 recites combining key splits to form a cryptographic key, initializing a cryptographic algorithm with the cryptographic key, and applying the cryptographic algorithm to an object, to form an encrypted object. In contrast, Lipner et al. disclose forming a cryptographic key, using the key to encrypt a message, and then splitting the key for further use. These are two entirely different processes.

The Examiner also cited Lipner et al. column 7, lines 40-43 as disclosing initialization of a cryptographic algorithm with a cryptographic key. The passage cited by the Examiner states that the Lipner et al. invention uses an unclassified data encryption algorithm. The passage does not describe initializing the algorithm with a cryptographic key, and particularly not with a cryptographic key formed by combining splits.

Lipner et al. disclose use of biometric tests for authentication, as noted by the Examiner, at column 21, lines 34-41. These tests are used as a replacement for, or in addition to, password-type authentication for access to a system. Lipner et al. do not disclose or suggest use of biometric correspondence to a cryptographic key split. Lipner at al. disclose that a public/private key pair KU can be seeded with external parameters, but there is no suggestion that biometric authentication data, as disclosed by Lipner et al., would correspond to an actual key split used to form the key, particularly since Lipner et al. does not form cryptographic keys from key splits.

For at least the foregoing reasons, the invention as recited in claim 1 is not rendered obvious by Lipner et al. Claims 2-6 depend from claim 1, and therefore also are not rendered obvious by Lipner et al. The rejection of claims 1-6, therefore, should be withdrawn.

Independent claim 21 recites a storage medium that includes instructions for causing a data processor to encrypt an object. The instructions include generate a cryptographic key by combining a plurality of key splits, initialize a cryptographic algorithm with the cryptographic key, and apply the initialized cryptographic algorithm to the object to form an encrypted object. At least one of the key splits corresponds at least in part to a biometric measurement.

The Examiner cited Lipner et al. as disclosing that a plurality of key splits is combined to generate a cryptographic key, citing column 15, lines 13-16. This passage discusses a multiple split session key, referring to Fig. 13, which shows the flow of a sending program. According to this program, a secret session key KS is negotiated and formed, and then used to encrypt a message M. It is not disclosed that this key is formed through the combination of key splits. After encryption of the message, the session key is split into multiple parts. The example mentions splitting the key into two halves KS1 and KS2. See column 14, lines 55-66. These are the split session keys mentioned in the passage cited by the Examiner.

Thus, claim 21 recites instructions to combine key splits to form a cryptographic key, initialize a cryptographic algorithm with the cryptographic key, and apply the cryptographic algorithm to an object, to form an encrypted object. In contrast, Lipner et al. disclose forming a cryptographic key, using the key to encrypt a message, and then splitting the key for further use. The Lipner et al. process is entirely different than the claimed instructions.

The Examiner also cited Lipner et al. column 7, lines 40-43 as disclosing initialization of a cryptographic algorithm with a cryptographic key. The passage cited by the Examiner states that the Lipner et al. invention uses an unclassified data encryption algorithm. The passage does not describe initializing the algorithm with a cryptographic key, and particularly not with a cryptographic key formed by combining splits.

Lipner et al. disclose use of biometric tests for authentication, as noted by the Examiner, at column 21, lines 34-41. These tests are used as a replacement for, or in addition to, password-type authentication for access to a system. Lipner et al. do not disclose or suggest use of biometric correspondence to a cryptographic key split. Lipner at al. disclose that a public/private key pair KU can be seeded with external parameters, but there is no suggestion that biometric authentication data, as disclosed by Lipner et al., would correspond to an actual key split used to form the key, particularly since Lipner et al. does not form cryptographic keys from key splits.

For at least the foregoing reasons, the invention as recited in claim 21 is not rendered obvious by Lipner et al. Claims 22-26 depend from claim 21, and therefore also are not rendered obvious by Lipner et al. The rejection of claims 21-26, therefore, should be withdrawn.

The Examiner rejected claims 7, 8, 10-28 and 30-40 under 35 USC §103(a) as being unpatentable over Sudia, in view of Lipner et al.

Independent claim 7 recites a method of encrypting an object by a user, in a cryptographic system associated with an organization. According to the claimed method, a first cryptographic key is generated by combining an organization split corresponding to the organization, a maintenance split, a random split, and at least one label split. A cryptographic algorithm is initialized with the first cryptographic key. The object is encrypted according to the initialized cryptographic algorithm. Combiner data is added to the encrypted object. The combiner data includes reference data corresponding to at least one of the at least one label split and the cryptographic algorithm, name data associated with the organization, the maintenance split and/or a maintenance level associated with the maintenance split, and the random split. The encrypted object is stored with the added combiner data

The Examiner cited Sudia at column 18, lines 65-67 as disclosing generation of a private key by combining key splits. That passage discusses the possibility of recombining splits of a private key in order to reassemble the private key. However, as noted, the private key is reassembled after the splits are recombined. Independent claims 1 and 21 recite generating a cryptographic key by combining key splits. As described in the section leading into the passage cited by the Examiner (column 17, line 29 through column 18, line 61), the disclosed invention utilizes a public/private encryption key pair. The private key is merely generated randomly by a firmware program (column 17, lines 50-61). Later, the generated private key is divided into a number of splits (column 18, lines 12-15) after the message has been encrypted and transmitted (column 17, line 65 through column 18, line 11).

The Examiner also cited column 10, lines 62-67 as disclosing the initialization of a cryptographic algorithm using a key. However, that passage merely describes that a known method is used to split private encryption keys into components.

The Examiner cited column 11, lines 33-39 as disclosing the addition of combiner data. That passage describes the use of a message control header that includes particular law enforcement information, but is not disclosed to include the reference data corresponding to key splits recited in claim 7. Likewise, Fig. 18 shows the message control header as described, including exemplary header components, but makes no correspondence between this data and key splits that are used to generate a key.

Thus, the Sudia invention is fundamentally different from the claimed invention. Some differences between Lipner et al. and the claimed invention are noted above. Neither reference satisfies the deficiencies of the other reference, with respect to the claimed invention. For at least all of the stated reasons, no combination of the teachings of Sudia and Lipner et al. could render obvious the invention recited in claim 7. Claims 8 and 10-20 depend from claim 7 and therefore also are not rendered obvious by the asserted combination. The rejection of claims 7, 8, and 10-20, therefore, should be withdrawn.

As discussed above, independent claim 21 is not rendered obvious by Lipner et al. Also as discussed, the teachings of Sudia do not overcome the deficiencies of the Lipner et al. disclosure. Therefore, no combination of the teachings of these two references could render obvious the invention as recited in claim 21. Claims 22-26 depend from claim 21, and therefore also are not rendered obvious by the asserted combination. The rejection of claims 21-26, therefore, should be withdrawn.

Independent claim 27 recites a storage medium comprising instructions for causing a data processor to encrypt an object. The instructions include generate a first cryptographic key by combining an organization split corresponding to an organization, a maintenance split, a random split, and at least one label split; initialize a cryptographic algorithm with the first cryptographic key; apply the initialized cryptographic algorithm to the object to form an encrypted object; add combiner data to the encrypted object and store the encrypted object with the combiner data for subsequent access. The combiner data includes reference data corresponding to at least one of the at least one label split and the cryptographic algorithm, name data associated with the organization, at least one of the maintenance split and a maintenance level corresponding to the maintenance split, and the random split.

The Examiner cited Sudia at column 18, lines 65-67 as disclosing generation of a private key by combining key splits. That passage discusses the possibility of recombining splits of a private key in order to reassemble the private key. However, as noted, the private key is reassembled after the splits are recombined. Independent claims 1 and 21 recite generating a cryptographic key by combining key splits. As described in the section leading into the passage cited by the Examiner (column 17, line 29 through column 18, line 61), the disclosed invention utilizes a public/private encryption key pair. The private key is merely generated randomly by a firmware program (column 17, lines 50-61). Later, the generated private key is divided into a number of splits (column 18, lines 12-15) after the message has been encrypted and transmitted (column 17, line 65 through column 18, line 11).

The Examiner also cited column 10, lines 62-67 as disclosing the initialization of a cryptographic algorithm using a key. However, that passage merely describes that a known method is used to split private encryption keys into components.

The Examiner cited column 11, lines 33-39 as disclosing the addition of combiner data. That passage describes the use of a message control header that includes particular law enforcement information, but is not disclosed to include the reference data corresponding to key splits recited in claim 7. Likewise, Fig. 18 shows the message control header as described, including exemplary header components, but makes no correspondence between this data and key splits that are used to generate a key.

Thus, the Sudia invention is fundamentally different from the claimed invention. Some differences between Lipner et al. and the claimed invention are noted above. Neither reference satisfies the deficiencies of the other reference, with respect to the claimed invention. For at least all of the stated reasons, no combination of the teachings of Sudia and Lipner et al. could render obvious the invention recited in claim 27. Claims 28 and 30-40 depend from claim 27 and therefore also are not rendered obvious by the asserted combination. The rejection of claims 27, 28, and 30-40, therefore, should be withdrawn.

The Examiner rejected claims 9 and 29 under 35 USC §103(a) as being unpatentable over Sudia, in view of Lipner et al., and further in view of Nguyen.

The Examiner relies on the teachings of Lipner et al. and Sudia as disclosing the elements of the claims as described above, and on Nguyen only for teaching that a key can be created from a user ID and password. The deficiencies of Lipner et al. and Sudia, and their combination, in disclosing the elements of independent claims 7 and 27 are discussed above. Nguyen does not overcome these deficiencies, nor does the Examiner assert that this is the case. Claims 9 and 29 depend from claims 7 and 27, respectively, and therefore no combination of the teachings of the asserted references could render obvious the invention as recited in claims 9 and 29. The rejection of claims 9 and 29, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all rejections have been overcome and all requirement have been satisfied. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

A petition for extension of time is enclosed, along with a check in payment of the fee for the extension. If the check is missing, or made out for an insufficient amount, please charge any deficiency to our deposit account, No. 501998, and notify us accordingly.

Respectfully submitted,

March 31, 2004
Date

Thomas M. Champagne
Registration No. 36,478
IP STRATEGIES, P.C.
1730 N Lynn Street
Suite 500
Arlington, Virginia 22209
703.248.9220
703.248.9244 fax